



Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 17 February 2004

Current Nationwide
Threat Level is



[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- CNET reports some California workers may have had their salaries and other personal information compromised after someone gained unauthorized access to a state agency's computer. (See item [8](#))
- The Associated Press reports U.S. Navy sailors may now board thousands of commercial ships in international waters to search for weapons of mass destruction, under a landmark pact between the U.S. and Liberia. (See item [17](#))
- The Associated Press reports agriculture officials have announced that a strain of bird flu, which is devastating to commercial chicken flocks but not harmful to humans, has spread from New Jersey into Pennsylvania and more cases may be found in Delaware. (See item [20](#))
- Government Computer News reports that code designed to exploit a recently announced critical vulnerability in Microsoft operating systems now is widespread on the Internet. (See item [33](#))

DHS/IAIP Update *Fast Jump*

Production Industries: [Energy](#); [Chemical](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [General](#); [DHS/IAIP Web Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

February 14, Associated Press — **Wolf Creek shuts down nuclear plant. Wolf Creek Generating Station in Burlington, KS, shut itself down Friday, February 13, due to an apparent equipment malfunction. Susan Maycock, a spokesperson at the nuclear power plant, said a preliminary review indicated a malfunction of the feedwater control system caused a loss of flow to one of four steam generators.** The plant automatically shut itself down as a result. "The plant is in a safe condition," said Rick Muench, president and chief executive officer of the plant, in a statement. Maycock said power from other plants was diverted to provide electricity to the customers served by Wolf Creek. She said it was not known when the plant would resume operations.

Source: http://www.dodgeglobe.com/stories/021404/sta_0214040069.shtml

2. *February 14, Associated Press* — **Electric grid still vulnerable six months after blackout. Six months after the nation's worst blackout, experts say the electric grid is still vulnerable to widespread outages because many of the problems that contributed to the massive failure have not been resolved.** "Without significant investment in the transmission system, we're all going to face another blackout. It's inevitable," according to Jonathan Smidt, an associate in the energy group of Kohlberg Kravis Roberts & Co., a private equity firm. **A repeat of the havoc wreaked on August 14, when outages in Ohio rapidly spread through seven other states and Canada, remains plausible so long as the industry remains "polarized" by regional interests and competing ideas about market design, both of which inhibit cooperation, said Lawrence Makovich, senior director at Cambridge Energy Research Associates.** "We've been grappling with the issue of how to maintain reliability as the market evolves," said Eugene McGrath, chairman and chief executive of Consolidated Edison, Inc. According to McGrath, the good news is that the areas of vulnerability are better known. That, in itself, reduces the risk of another cascading blackout, he said.

Source: <http://www.mcall.com/business/local/all-blackoutfeb14.0,3787493.story?coll=all-businesslocal-hed>

[\[Return to top\]](#)

Chemical Sector

Nothing to report.

[\[Return to top\]](#)

Defense Industrial Base Sector

3. *February 14, Associated Press* — **Air Force launches rocket carrying missile-detection satellite. A Titan 4B rocket took off from Florida Saturday, February 14, carrying an Air Force satellite that will give the U.S. military an early warning of incoming missile attacks.** The Defense Support Program satellite has a life expectancy of at least 10 years. The rocket will place the satellite into a geosynchronous orbit 22,300 miles above the earth about seven hours after liftoff. **Defense Support Program satellites use infrared sensors to detect heat from missile and booster plumes against the earth's background.** The program began in the early 1970s and improvements since then have made the system more sensitive. Since the mid-1990s, upgrades have allowed the satellites already on orbit to detect smaller missiles,

giving ground commanders more time to react to short-range missile attacks. Military officials said that missile threats exist in the former Soviet Union and in other nations. "They're all over the world and we see nations and other elements that are willing to use them, so we think we still need the capability," said Col. Robert S. Reese, deputy program manager for Space Based Infrared Systems.

Source: <http://www.theledger.com/apps/pbcs.dll/article?AID=/20040214/APN/402140742>

4. *February 12, Govexec.com* — **Defense expects a 'global' round of base closings in 2005. The Department of Defense will announce within the next 90 days a realigning of forces overseas that will have a major impact on which bases in the United States will be marked for closure in 2005, according to Raymond Dubois, deputy undersecretary of Defense for installations and environment. Dubois told the House Appropriations Military Construction Subcommittee on Thursday, February 12, that the 2005 round of military base realignment and closures (BRAC) would be a "global BRAC." The ongoing review of overseas bases will have a major impact on forces based stateside.** For example, Dubois said, the Army might bring a division, about 10,000 soldiers, home from Germany, and the service would then decide where to base them in the U.S. Dubois said the 2005 plan has several changes from past BRAC rounds, including: having nine commission members rather than eight to prevent tie votes; relying on a 20-year force structure plan instead of a six-year plan for deciding which bases are needed; and creating joint working groups work groups at the Pentagon to consider where services may consolidate common functions.

Source: <http://www.govexec.com/dailyfed/0204/021204g1.htm>

[[Return to top](#)]

Banking and Finance Sector

5. *February 13, Reuters* — **Anti-spam scam mimics official site. An official-looking Website promising to reduce spam may itself be collecting e-mail addresses for spammers, the U.S. Federal Trade Commission (FTC) has warned.** Consumers should not submit their e-mail addresses to a Website that promises to reduce unwanted "spam" because it is fraudulent, the FTC said on Thursday, February 12. **Though the Website, found at www.unsub.us, professes to minimize unsolicited commercial e-mail, those who sign up could end up receiving more spam than ever or even fall victim to identity theft,** the FTC said. The unsub.us Website is not affiliated with the government and consumers should not submit their e-mail addresses to the site, the FTC said in a news release.

Source: <http://news.zdnet.co.uk/internet/security/0.39020375.3914618.0.00.htm>

6. *February 13, Russian Information Agency Novosti* — **Kremlin dissatisfied with anti-money laundering efforts. In 2003, no cases of laundering of money earned by drug-dealing, arms-dealing and prostitution were exposed in Russia, Deputy Kremlin Chief-of-Staff Viktor Ivanov said** at an extended Interior Ministry Board session Friday, February 13. **According to Ivanov, only 14 money laundering cases were sent to court last year, however half of them were closed due to lack of evidence.** The damage done by such crimes in Russia amounts to billion dollars, according to the Central Bank data. "The analysis of the situation suggests that organized criminal groups earn part of that amount from drug-dealing and illegal migration. It is also possible that this money is used to finance terrorist activities,"

Ivanov went on to say.

Source: http://en.rian.ru/rian/index.cfm?prd_id=160&msg_id=3926780&sttartrow=1&date=2004-02-13&do_alert=0

7. *February 13, Air Force Press News* — **Changes to statements may reduce identity theft.** Leave and earning statements for all servicemembers and Department of Defense civilians, and paychecks for military retirees will soon have more identity theft protection. **Over the next several weeks, the Defense Finance and Accounting Service will drop the first five digits of a person's Social Security number from all pay statements and checks to guard against identity theft.** This change is due to reports that identity theft has substantially increased in recent years, according to the Federal Trade Commission, which monitors the issue.
Source: <http://www.af.mil/news/story.asp?storyID=123006979>
8. *February 13, CNET* — **State agency warns of security breach.** Some California workers may have had their salaries and other personal information compromised after someone gained unauthorized access to a state agency's computer. **The California Employment Development Department (EDD) has begun warning some current and former household workers that their information may have been accessed by an intruder.** The agency sent a letter, dated February 11, notifying people of the breach and offering information about how to reduce the risk of identity theft. **Approximately 55,000 employees were affected, EDD spokesperson Kevin Callori said. The agency said the database in question contained names, Social Security numbers and wages.** Callori said that the breach, which was detected on January 20, was limited to a single server containing information about household workers. "There is no evidence they accessed personal information," he said. "Apparently, they were using the server to send out spam," Callori added.
Source: <http://news.com.com/2100-7355-5158936.html>
9. *February 12, Australian IT* — **Ticketer lashed for security hole. Ticketmaster 7 has been criticized by the Australian Federal Privacy Commissioner for a flaw in its Website which allowed anyone to look up personal information entered by other users. The flaw was in one of the ticketing company's Website services, which allowed users to make enquiries.** Each query was assigned a URL with a unique four-digit number to track the changes in their session, but any user could change those digits and find another user's name, address, and e-mail address. Ticketmaster 7 told the commission it closed down the service Thursday, February 11, and checked that the problem did not affect its other Website services. The company also said it would address quality management of its IT infrastructure in more detail.
Source: <http://australianit.news.com.au/common/print/0,7208,8660706%5E15331%5E%5Enbv%5E15306%2D15318,00.html>

[\[Return to top\]](#)

Transportation Sector

10. *February 16, Associated Press* — **Amtrak says new budget will shut down railroad.** The head of Amtrak says President Bush's proposed budget will shut down the railroad. **Amtrak President David Gunn says the president's proposed 900 (M) million dollar budget is a**

"shutdown" number that comes just as the railroad is attracting new passengers. The amount is just over half what Amtrak asked for. The administration is acknowledging Amtrak's improved performance but says more change is needed. A statement says the administration would support an additional 500 (M) million if major reforms are made. Gunn says he expects 25 million people will ride Amtrak this budget year, breaking the previous record of 24 million.

Source: <http://www.kltv.com/Global/story.asp?S=1639058>

11. *February 16, Associated Press* — **German airport introduces iris scan. Travelers at Germany's Frankfurt airport, continental Europe's busiest, can now enter Germany with a three-second scan of their eyes, providing they sign up for a test project for iris recognition technology.** Passengers in the six-month program still go through regular security controls, but can bypass conventional passport checks. They can simply put their passport through a scanner, take a quick look at a camera and a few seconds later enter the country, airport officials said. To qualify, passengers would need background checks by German border police, a machine-readable passport, be citizens of the European Union or Switzerland, register at the airport and have an iris scan on file. **The test is part of efforts in many countries, especially the United States in the wake of the September 11 attacks, to extend the use of biometric technology -- using fingerprint, eye or facial recognition scans -- to track travelers and immigrants, while also cutting down on time spent in line. Post-September 11 U.S. legislation also requires 27 countries, mostly in Europe, to add biometrics to passports they issue after October 26, 2004, or else have their citizens apply for visas.**

Source: <http://www.cnn.com/2004/TECH/ptech/02/16/irisscan.airport.ap/index.html>

12. *February 16, CNN* — **Grenade found in car entering U.S. On Monday, February 16, Canadian border patrol officials found a grenade in the glove compartment of a car that was trying to enter the United States, Canadian authorities told CNN, forcing a brief closure of the crossing between Blaine, WA, and White Rock, British Columbia.** The car was driven by a 28-year-old woman who said her husband, who is serving in the military, just got back from Iraq, according to Royal Canadian Mounted Police (RCMP) spokesperson Tim Shields. Canadian Border Guard Agency spokesperson Paula Shore said the incident will be investigated, but it appears to be innocent. "After speaking to my colleagues at the RCMP, they're quite satisfied that this is just something that was a mistake," she told CNN's Wolf Blitzer. An RCMP explosives disposal unit removed the grenade from the car and secured it, Shore said. The border crossing was closed around 1 p.m. PT (4 p.m. ET) and re-opened about an hour later, officials said. "We don't take chances at the border," Shore said.

Source: <http://www.cnn.com/2004/US/02/16/border.grenade/index.html>

13. *February 15, The Miami Herald* — **Concerns mount over safety of gas tankers.** Tankers carrying millions of gallons of liquefied natural gas move in and out of harbors protected by an armada of ships and helicopters. But many worry that's not enough. At 930 feet long, the Inigo Tapias is one of the largest ships to do business in the harbor. Stood on end, it would dwarf the city's tallest building, the 750-foot John Hancock tower. And its cargo is certainly the most menacing. **Every few days, tankers like this one carry 33 million gallons of liquefied natural gas to a plant in Everett. They pass within a few hundred yards of downtown Boston and Logan Airport, where terrorists hijacked two planes and torpedoed them into the World Trade Center.** With September 11, 2001, in mind, the Coast Guard coordinates an

armada of protection for each trip — a helicopter, police divers, marine patrol, environmental police, firefighting tugs, city police boats, Coast Guard vessels. The Tobin Bridge, a major commuter pass, is closed as the tankers move below its 135-foot-high span. **Heightened fears of terrorism and a recent surge in proposals to build dozens of gas terminals around the United States have raised questions about whether they're too dangerous for metropolitan areas.** Boston is one of just four ports in the continental United States to receive liquefied natural gas by ship, and the only one in a commercial and residential hub.

Source: <http://www.miami.com/mld/miamiherald/news/nation/7957774.htm>

14. *February 15, The Post and Courier (Charleston, SC)* — **Partnerships and alliances take off in the airline industry.** The airline industry is more competitive than ever, with big carriers scrapping for market share while trying to fend off a growing crop of discounters. At the same time, the industry is working more cooperatively than ever, with battle-scarred veterans increasingly selling tickets on each others' planes to stay alive. **It's called code sharing, and it is letting some of the big carriers stay viable without having to resort to consolidation.** Code sharing became more evident in 1989, when Northwest Airlines teamed up with Netherlands-based KLM Royal Dutch Airlines. **By 1998, four of the country's biggest carriers had paired off in domestic alliances to expand their offerings. Northwest teamed up with Continental Airlines, and United Airlines and Delta Air Lines announced similar plans a couple months later.** The Department of Transportation (DOT) reviews all code sharing between major domestic carriers to see whether the proposed partnerships will hurt competition. DOT has forced carriers to tweak a few requests, but it has never turned any down completely. Analysts laud the partnerships as a win-win, benefiting both passengers and carriers.

Source: http://www.charleston.net/stories/021504/bus_15planes.shtml

15. *February 13, Department of Transportation* — **Federal Railroad Administrator announces \$4.6 million loan to the Stillwater Central Railroad.** The Stillwater Central Railroad, Inc. of Stillwater, OK will receive a \$4.6 million federal loan from the Federal Railroad Administration to increase the reliability of rail services for regional railroad customers in central Oklahoma. **U.S. Secretary of Transportation Norman Y. Mineta stressed the role of regional railroads in growing the nation's economy. "Moving freight moves the economy. Americans profit from dependable, efficient, and safe transportation as we ship goods throughout America."** The Stillwater Central Railroad is a short line railroad that operates freight services over approximately 120 miles of rail lines in Oklahoma. It serves well-established bulk commodity companies including the largest gypsum mine in the United States. With a traffic base of 20 shippers, the railroad carried an estimated 17,000 carloads of products in 2003. The 25 year loan will be used to refinance existing debt incurred during the purchase of a rail line from the Burlington Northern Santa Fe Railroad and to buy a locomotive.

Source: <http://www.dot.gov/affairs/fra0304.htm>

16. *February 13, Department of Transportation* — **Cruise passenger travel grows eight percent.** The top ten cruise lines carried 8.3 million passengers on 3,840 North American cruises in 2003, up eight percent over 2002, the U.S. Maritime Administration (MARAD) reports. The highest growth rates among the top ten departure ports occurred in New York and Galveston, which recorded increases of 45 percent and 39 percent respectively in 2003. However, the traffic remains heavily concentrated at the major departure ports, which are located in Florida.

Miami, Port Canaveral, and Fort Lauderdale accounted for 49 percent of the total cruise passenger traffic. **The figures are part of a statistical series issued quarterly by MARAD on U.S. cruise passenger traffic, with data for the 10 major cruise lines operating cruise ships with a capacity greater than 750 passengers.**

Source: <http://www.dot.gov/affairs/marad504.htm>

17. *February 13, Associated Press* — **Pact lets U.S. search Liberia-flagged ships for WMDs. U.S. Navy sailors may board thousands of commercial ships in international waters to search for weapons of mass destruction under a landmark pact between the United States and Liberia, the world's No. 2 shipping registry.** This accord — expected to become a model as Washington seeks other two-country deals authorizing searches on the high seas — comes amid fears that terror networks would use ships for attacks, taking advantage of comparatively lax security on the waters after crackdowns in the skies. **Liberia ranks second only to Panama in total shipping tonnage in U.S. ports, under so-called flags of convenience that offer cheap fees and easy rules. One-third of America's imported oil arrives in the United States on Liberian-flagged tankers.** With the pact, American forces may board and search any Liberian-registered foreign ship they suspect of carrying weapons of mass destruction, their delivery systems, or related material, State Department spokesperson Richard Boucher said in Washington.

Source: <http://www.cnn.com/2004/WORLD/africa/02/13/liberia.shipsearc.hes.ap/index.html>

[[Return to top](#)]

Postal and Shipping Sector

Nothing to report.

[[Return to top](#)]

Agriculture Sector

18. *February 16, Associated Press* — **Standing firm on U.S. beef ban, Japan wants a new probe. Japan's agriculture minister Saturday called a U.S. probe into the outbreak of mad cow disease incomplete and said his country would not reconsider a six-week ban on American beef until it receives new proposals from the U.S. for tighter safeguards.** Japan is pressing the U.S. to test all cattle for the disease before slaughter, a measure implemented by Japan's much smaller beef industry after a mad cow scare there two years ago. The U.S. says blanket testing is unnecessary and would be prohibitively expensive, but a series of U.S. agriculture and trade officials sent to Tokyo to persuade Japan to lift an import ban have come away empty handed. Agriculture Minister Yoshiyuki Kamei said Saturday that he had asked the most recent delegation to propose safeguards "based on" Japan's system, which Kamei credited with restoring consumer confidence in Japanese beef. **Before it suspended imports on December 24, Japan was the most lucrative export market for U.S. beef, buying almost \$1 billion worth in 2002.**

Source: <http://www.taipeitimes.com/News/worldbiz/archives/2004/02/16/2003099014>

19.

February 16, Voice of America — **Bird flu resurfaces.** The bird flu that has spread through chickens and killed at least 20 people in Asia has recurred in Thailand in places where it had previously been contained. **Thailand's Deputy Agriculture Minister Newin Chidchop says new outbreaks of the bird flu have occurred in nine Thai provinces. In eight of those provinces, the government had thought the disease was contained, after it had culled thousands of chickens.** At least 10 Asian countries have confirmed outbreaks in poultry, although some of them have a milder type of the disease.

Source: <http://www.voanews.com/article.cfm?objectID=84891B4D-F685-434B-92876C5BB777AEBD>

20. *February 12, Associated Press* — **Bird flu found in two more states. A strain of bird flu which is devastating to commercial chicken flocks but not harmful to humans has spread into Pennsylvania and more cases may be found in Delaware, agriculture officials in both states said on Thursday.** The disease was also confirmed in four small poultry markets in northeastern New Jersey, a state which has had the disease for a dozen years and does not have any large, commercial flocks, according to its state officials. Chicken accounts for one-third of U.S. meat consumption. **The Pennsylvania infection was found in a flock of nearly 500,000 egg-producing hens, which was immediately quarantined. The birds, which have not shown any physical signs of illness, may be destroyed depending on further testing.** Some 16 poultry flocks within a two-mile radius of the infected Pennsylvania farm will undergo testing for the virus. Farmers fear the disease because it can rapidly spread throughout a flock, cutting egg production and producing misshapen or soft-shelled eggs.

Source: <http://news.myway.com/top/article/id/383848|top|02-12-2004::17:12|reuters.html>

21. *February 12, Purdue University* — **Engineers create chip-size version of widely used detector.** Researchers have created a portable, chip-size version of a detection system that is commonly used to identify everything from agricultural toxins to DNA. **The miniature detector could move certain types of testing from the lab into the field, saving time and money while increasing security.** The traditional fluorescence detection system works by attaching a fluorescent dye to specific molecules in a substance and then shining a laser onto the substance. The laser light is absorbed by the dyed molecules, causing them to emit a certain color, which is picked up by a sensor. The detection work normally is done using bulky, stationary equipment in a laboratory. The new device, however, fits on a centimeter-wide chip, promising the development of miniature detectors that can be used in the field. **Such portable instruments would be useful for a wide range of applications, from biologists doing basic research to farmers testing crops for toxins.**

Source: <http://www.ascribe.org/cgi-bin/spew4th.pl?ascribeid=20040212.124205&time=13%2011%20PST&year=2004&public=1>

[[Return to top](#)]

Food Sector

22. *February 14, Associated Press* — **Panel urges increased mad cow testing.** A federal panel suggested that the U.S. government step up testing for mad cow disease to evaluate any risk to American consumers. Members of the U.S. Food and Drug Administration panel made the recommendation Friday at a meeting in Maryland. In December, a cow from a Mabton, WA,

dairy became the first U.S. animal to test positive for bovine spongiform encephalopathy, or mad cow disease. "We have to know what the risk is, and whether we could contain it or whether we could stop it," said panelist Stephen DeArmond, a mad cow disease expert at the University of California. The U.S. Department of Agriculture has said it has planned to test 40,000 out of 35 million cows to be slaughtered this year, with an emphasis on cows at high risk for the disease. **The panelists said testing a greater number of cows was necessary to determine whether cosmetics, dietary supplements, drugs, and the blood supply are adequately protected from the disease.**

Source: <http://www.centredaily.com/mld/centredaily/news/7955140.htm>

[\[Return to top\]](#)

Water Sector

23. *February 13, Water Tech Online* — **EPA: Water utilities want more security support.** U.S. water utilities want more security information and more training and financial assistance to support security initiatives, according to a survey by the Environmental Protection Agency's (EPA) Inspector General. The EPA surveyed 16 water systems in six states about their security needs. **The EPA found that water systems received most of their information on threat identification, problem detection, delay barriers, response capabilities, and computer control systems from consultants, the American Water Works Association and the EPA.** The survey also found that 11 of the 16 utilities estimated they would spend more than \$100,000 in the next year on security improvements, with four estimating their security expenses would top \$1 million. Of the 16 surveyed systems, four serve 3,300 to 99,999 people and 12 serve 100,000 or more, while 14 have completed mandated vulnerability systems and 15 employed consultants to do so.

Source: http://www.watertechonline.com/news.asp?mode=4&N_ID=46019

[\[Return to top\]](#)

Public Health Sector

24. *February 15, Associated Press* — **Over 300 sickened on cruise to Mexico.** A Carnival Cruise Lines ship returned from a five-day cruise to Mexico on Saturday with more than 300 people sick with a gastrointestinal illness. **Carnival officials said preliminary tests show the outbreak might have been caused by a norovirus.** The virus is spread through contaminated food, contact with infected people, or poor hygiene. The Celebration left Galveston on Monday. On Wednesday, Carnival contacted the U.S. Centers for Disease Control and Prevention (CDC) to report an unusual number of ill passengers, with predominant symptoms of vomiting and diarrhea. By Friday, 297 of 1,576 passengers and 19 of 689 crew members were ill. CDC investigators boarded the ship after its regularly scheduled arrival. They were conducting tests and inspecting the ship.

Source: <http://www.newsmax.com/archives/articles/2004/2/15/102357.sh tml>

25. *February 13, CanWest News Service* — **Pandemic plan predicts up to 58,000 deaths.** Canada needs to make vaccines faster, and have plans for temporary morgues with

volunteer gravediggers, if it hopes to combat an "overdue" pandemic flu outbreak, says the new Canadian Pandemic Influenza Plan. Such an outbreak would force health authorities to re-shape virtually everything they do to treat illness and keep society stable, says the plan. For instance, flu victims would have to go somewhere after hospitals and doctors' offices are full. And this will mean setting up "non-traditional" health-care sites in schools, community centers, churches, banquet halls, and daycare centers. "We believe we are overdue" for the next flu pandemic, Arlene King of Health Canada said Thursday as the plan was unveiled. That doesn't mean anyone can foresee when it will hit. What's more certain is there would be little warning. If the normal flu bug evolves into something nastier, if no vaccine is available, a pandemic could kill 11,000 to 58,000 Canadians and make 2.1 million to five million ill. Vaccines are to be Canada's main line of defense. The plan outlines a guaranteed system under which a pharmaceutical company has contracted with Health Canada to make enough vaccine for every Canadian. But it would take months to make any vaccine doses, and up to a year to make enough for the whole population.

Source: <http://www.canada.com/health/story.html?id=50BB7A3B-A8DA-4ACD-93F5-E5738E6ECC4D>

26. *February 12, United Press International* — **WHO probes viral deaths in Bangladesh.** World Health Organization (WHO) officials said Thursday they were investigating an outbreak of a Nipah-like virus in Bangladesh that has led to 14 deaths. Nipah virus, first identified in Malaysia in 1999, is thought to be carried by an animal, perhaps bats, cats, dogs, and pigs. **WHO said from January 4 to February 8 at least 42 cases and 14 deaths in the Manikganj and Rajbari provinces of Bangladesh have been attributed to a virus that appears to be similar to the Nipah pathogen.** The U.S. Centers for Disease Control and Prevention has confirmed a Nipah-like virus in nine of the cases. Forty-five other cases were being investigated by an international team comprised of experts from WHO, the United States, France, and Bangladesh. Many cases of Nipah infection are mild, but in other cases the disease can lead to inflammation of the brain, coma, and death. There is no treatment.

Source: <http://washingtontimes.com/upi-breaking/20040212-010329-8074 r.htm>

[[Return to top](#)]

Government Sector

Nothing to report.

[[Return to top](#)]

Emergency Services Sector

27. *February 16, Port Clinton News Herald (Ohio)* — **Ohio county weighs options for use of Homeland Security grants.** Fred Peterson, of the Ottawa County (Ohio) Emergency Management Agency, said his department has received **federal funding in five stages to be spent on preparing Ottawa County for biological and chemical emergencies, such as terrorist attacks, chemical spills from train derailments or weapons of mass destruction being deployed in or near Ottawa County.** Peterson said the biggest purchase so far for Ottawa County is the acquisition of two large, portable decontamination units. One of these

blow-up domes is housed at Magruder Hospital and one is at the Allen–Clay Fire Department. The team also approved a \$40,000–purchase of chemical protection kits, including respirators and gloves, that were given to most police departments, the sheriff's office and EMS teams. He said there are several reasons the money is needed. **For example, if a biological attack, such as a weapon of mass destruction, hit Toledo or another surrounding city, Ottawa County would have to be prepared to help, he said. Also, Peterson said Davis–Besse Nuclear Power Station puts Ottawa County at a higher risk of a nuclear emergency. Also, he said, the railroad is a hazard because cars carrying chemicals could spill.**

Source: <http://www.portclintonnews herald.com/news/stories/20040216/1ocalnews/425160.html>

28. *February 15, Clovis News Journal (Texas)* — Hospital: Hazmat mishap mishandled.

Communications problems which complicated an emergency medical run on February 2 could have implications for any future disaster, members of the exercise design subcommittee of the Curry County (Texas) Local Emergency Planning Committee noted Friday, February 13. On that day, a train crew member was taken to Plains Regional Medical Center after inhaling denatured alcohol mist seeping from a train stopped 10 miles west of Melrose. Terri Marney, director of quality assurance at the hospital, said **due to miscommunications, the hospital received incorrect information about what chemical had sickened the train crew member and refused to let the Melrose Fire Department bring the injured man into the hospital until the chemical was properly identified. “Our biggest problem is communication,” Marney said. “We had a real problem with lack of communication and a fire department that had no capability of doing decontamination.”** Committee members didn't come to a consensus on a solution, but some noted that radio reception in outlying areas is poor and the rural departments need not only better training but also upgraded equipment to respond effectively to emergencies.

Source: http://cnjonline.com/engine.pl?station=clovis&template=story_full.html&id=4480

29. *February 15, New York Times* — New York police take broad steps in facing terror. The New York Police Department, working with city health officials, federal authorities and other agencies, has been preparing for a possible attack with nuclear, biological or chemical weapons, perhaps the most daunting threat facing municipalities in a post–9/11 world. Police officials say special units have trained and drilled, for instance, to board cruise ships from helicopters and piers and have begun reviewing floor plans of most large Midtown theaters, conducting exercises inside some to improve their ability to respond to a possible attack, in the aftermath of the deadly siege of a Moscow theater two years ago. This spring, city and federal officials say, the police will work alongside the city health department and other agencies to open a pilot program that they hope will ultimately allow officials to test the air across the city for biological agents quickly and constantly. The Police Department has also begun to prepare for its role in a sweeping citywide plan to get antibiotics or vaccine to every resident after a widespread attack with biological weapons, and is drafting security plans for about 200 sites that could function as distribution centers.

Source: <http://www.nytimes.com/2004/02/15/nyregion/15THREAT.html?hp>

30. *February 15, Washington Post* — District to test emergency transmission network. The District of Columbia is beginning a pilot program for emergency communications that government officials hope could become a template for cities around the country. **The government will install a private wireless network somewhat similar to a cellular–phone**

network for police, fire and other emergency workers that will allow high-speed video, database and voice transmission inside the Capital Beltway. The \$2.7 million trial program will last for a year. About 200 people from public safety agencies and Washington Metropolitan Area Transit Authority will be allowed to connect to the network on their laptops and handheld computers during the trial period, the city said. "Washington is the first city to have the whole city covered with this high-speed mobile data network" for public safety use, said Suzanne Peck, the District's chief technology officer. If successful, she said, she hopes the idea will be repeated in cities across the country. Getting reliable and secure communications is essential in emergency situations to coordinate emergency response, Peck said. **Cellular and conventional telephone systems often get clogged when disaster strikes, which is why it is necessary to set up the city's own communications system.**

Source: <http://www.washingtonpost.com/wp-dyn/articles/A38246-2004Feb 12.html>

31. *February 14, Greeneville Sun* — Police unit destroys 'chemical bomb' placed in mailbox.

The Greeneville, TN, Police Department's bomb disposal unit on Friday afternoon, February 13, destroyed what officers said was a chemical bomb that had been placed in the mailbox of an Asheville Highway residence. A Greene County 911 spokesperson said the device was discovered and reported to 911 at 1:27 p.m. Friday. The police department's bomb-disposal unit responded to the scene. Also responding were a Greene County-Greeneville Emergency Medical Services (EMS) ambulance and a unit of the Greeneville Fire Department. "Two officers gingerly removed what proved to be a cylindrical potato-chip can wrapped in tape from the mailbox by attaching a string to it and pulling it onto the street and into a ditch on the opposite side of Sunrise Drive from the mailbox. **After the container was blown open, Officers said the potato-chip can had contained a mixture of chemicals that, if prepared properly, would have built up pressure until the container exploded.** Such devices, the two officers said, often are used by vandals to blow apart mailboxes.

Source: <http://www.greene.xtn.net/index.php?table=news&template=news.view.subscriber&newsid=108533>

32. *February 11, Government Technology* — Hazardous materials inventory information.

Citizens will be better informed and emergency personnel better prepared to respond with the launch of a new Web-based computer system that streamlines the submission and management of hazardous material inventory information. **Maryland's Online Tier II Reporting system (also known as the Tier II Manager) is an effort of the Maryland Department of the Environment's (MDE) Community Right-to-Know program.** "Until now, Maryland has kept this information in hard copy format, which meant the valuable chemical data was unavailable except during regular business hours," said MDE Acting Secretary Kendl P. Philbrick. "The Tier II Manager will provide emergency response personnel with access to this information 24 hours a day in an easy-to-use geographic information system and nearly eliminate the paper glut associated with submitting this crucial information to authorities." Since 1987, under federal guidelines, any facility that stores or uses above a certain quantity of a hazardous substance must submit a Tier II Emergency and Hazardous Chemical Inventory Report each March 1.

Source: <http://www.govtech.net/news/news.php?id=88688>

Information and Telecommunications Sector



33. *February 16, Government Computer News* — **Exploit code for Microsoft vulnerability circulating.** Security researchers say code designed to exploit a recently announced critical vulnerability in Microsoft operating systems now is widespread on the Internet. **The code crashes targeted computers by exploiting a flaw in Microsoft's Abstract Syntax Notation 1 Library in Windows NT, 2000 and XP.** The exploit code was discovered Saturday, February 14, four days after the vulnerability and a patch to correct it was announced by Microsoft. The code is available on several discussion groups and Web sites. Ken Dunham of iDefense Inc. said there have been reports of denial-of-service attacks against specific targets using this exploit, but the attacks are not yet widespread. "It may be a few days before we see anything beyond a DOD attack," he said. "Several attackers are actively working on an ASN.1 exploit to spread Trojans and 'bots. One attacker has expressed an interest in creating a worm that will 'take down the Internet.'" Dunham said the malicious actors are capable of "weaponizing" the exploit, but have so far had little success in their tests. In other malicious-code news, **Symantec Corporation has raised the security level for the new Welchia worm because of increasing numbers of infections.** Welchia, also known as Nachi, first appeared last August in the wake of the MSBlaster worm. It automatically patched against the vulnerability exploited by Blaster. **The new version, Welchia.b, appears to remove the MyDoom a and b worms from infected machines. Once installed on a machine, it tries successively to exploit three vulnerabilities against a random IP address.**

Source: http://www.gcn.com/vol1_no1/daily-updates/24946-1.html

34. *February 14, Associated Press* — **Belgium police arrest female virus-writer. Belgian police arrested a 19-year-old female technology student who gained international notoriety for creating computer viruses,** it was reported Saturday, February 14. The woman, identified only by her nickname "Gigabyte," was charged with computer data sabotage under legislation introduced in 2000 to deal with cyber-crime, the daily La Libre Belgique reported. If convicted, she faces up to three years in prison and fines of up to \$127,000. Police reportedly released the woman after 24 hours, confiscated her five computers and shut down her Website. She was arrested Monday in her hometown of Mechelen, 20 miles north of Brussels. "She was preparing to publish new viruses on this site," Inspector Olivier Bogaert of the Belgium police was quoted as telling La Libre Belgique. Her youth and gender helped gain Gigabyte notoriety in the male-dominated world of computer hackers. **In a 2002 interview Gigabyte defended her work, saying she herself never spread the viruses she created and published on her Website.** "When people make guns, can you blame them when somebody else kills with them?" she was quoted asking. "I only write them. I don't release them."

Source: <http://securityfocus.com/news/8048>

Internet Alert Dashboard

Current Alert Levels	
 AlertCon: 1 out of 4 https://gtoc.iss.net	 Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/
Current Virus and Port Attacks	
Virus:	#1 Virus in the United States: WORM_LOVGATE.G Source: http://wtc.trendmicro.com/wtc/wmap.html , Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	3127 (mydoom), 80 (www), 135 (epmap), 445 (microsoft-ds), 6129 (dameware), 137 (netbios-ns), 1080 (socks), 1434 (ms-sql-m), 3128 (squid-http), 4000 (Connect-BackBackdoor) Source: http://isc.incidents.org/top10.html ; Internet Storm Center

[[Return to top](#)]

General Sector

35. *February 16, International Herald Tribune* — **Iraqi police seize number 41 on the U.S. wanted list.** A former Baath Party chairman, No. 41 on the U.S. military's most-wanted list, was arrested by Iraqi police officers on Sunday, a senior Iraqi official said. **The former chairman, Muhammad Zimam Abdul-Razaq, was arrested at one of his homes in western Baghdad, said the official, Ahmed Kadhum Ibrahim, the deputy interior minister.** When Saddam Hussein was president, Abdul-Razaq was the Baath Party regional chairman in the northern provinces of Nineveh and Tamim. Ten fugitives from the list are still at large, and the U.S. military has offered a \$1 million reward for each of them.
Source: <http://www.ihf.com/articles/129709.htm>
36. *February 14, CNN* — **Gunfire hits SUV near Columbus, Ohio.** A sport utility vehicle on Interstate 70 in Granville, OH, was shot at on Saturday, February 14. Police think the incident appears to be linked to 23 previous sniper-style shootings in the Columbus area. No one was hurt in the shooting, which happened around 10:15 a.m. in an eastbound lane west of Highway 310, 20 miles east of Columbus, said Pat Snelling, a dispatcher with the Ohio Highway Patrol's Granville patrol post. **The driver of the SUV described the shooter as a clean-shaven white man in his 30s who was driving a black compact car similar to a Geo Metro, Snelling said.** Authorities in Ohio have linked the previous 23 shootings on or near the southwest corridor of Interstate 270, which circles Columbus. Gail Knisley, 62, was killed November 25 when a bullet pierced her car window as she rode on 270. No other injuries have been reported. The most recent shootings happened February 8. No one was injured in those two shootings, which happened at two interstate overpasses about a mile from each other around 11:20 a.m. ET. In each case, a bullet struck the driver's-side hood of vehicles traveling northbound on Interstate 71 southwest of Columbus. The shootings took place within minutes of each other. **Franklin County Sheriff Chief Deputy Steve Martin said last week that the daylight incidents are signs that the shooter is becoming more brazen.**

Source: <http://www.cnn.com/2004/US/Midwest/02/14/ohio.shootings/index.html>

[\[Return to top\]](#)

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web-site (<http://www.nipc.gov>), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings – DHS/IAIP Assessments, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications – DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive – Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions: nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at (703)883-3644

Subscription and Distribution Information: Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703-883-3644 for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call (202)323-3204.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open-source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.